# DEPARTMENT OF STATE

# PRIVACY IMPACT ASSESSMENT

## American Citizen Services Plus
## (ACS+)

**Conducted by:**
Bureau of Administration
Information sharing and Services
Office of Information Programs and Service
Privacy Office
Email: pia@state.gov

# The Department of the State
# Privacy Impact Assessment for IT Projects

## Introduction

The E-Government Act of 2002 (section 208) imposes new requirements on Government agencies to ensure that system owners and developers consider and evaluate existing statutory and key information management requirements that must be applied to new or modified Government systems that contain personal information.

The purpose of the new *****requirements is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government. Section 208 of the E-Government Act requires that agencies now conduct Privacy Impact Assessments (PIA) on all IT projects being planned, developed, implemented, and/or operating regarding individual agency information management systems. The Office of Management and Budget (OMB) has oversight of all federal agency implementation of the Privacy Act of 1974, as amended. OMB will be scrutinizing IT project budget requests based on this new requirement among those already in place. A completed PIA is also required for DOS Information Technology (IT) Security Certification and Accreditation (C&A).

The Office of Information Programs and Services is responsible for the Department-wide implementation of the Privacy Act. This Office will provide assistance in completing the assessment and will present its findings and suggestions in a report for your submission to OMB and/or other appropriate parties.

The goals accomplished in completing a PIA include:

- Providing senior DOS management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;
- Ensuring accountability for privacy issues with system project managers and system owners;
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy; and
- Providing basic documentation on the flow of personal information within DOS systems for use and review by policy and program staff, systems analysts, and security analysts.
- Going through the PIA process will also help to identify sensitive systems so that appropriate information assurance measures are in place, such as secured storage media, secured transmission and access controls.

***** These requirements are drawn from the Privacy Act, Computer Security Act, the Clinger-Cohen Act, the Government Paperwork Reduction Act, the Freedom of Information Act, and Office of Management and Budget (OMB) Circulars A-130: Management of Federal Information Resources and A-123: Management Accountability.

## Definitions

***Personal Information*** - Personal information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;
- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, address, telephone number, fingerprints, blood type, or DNA.

***Accuracy*** with respect to information that is capable of verification or susceptible of proof, within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

***Completeness*** - all elements necessary for making a determination are present before such determination is made.

***Determination*** - any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

***Necessary*** - a threshold of need for an element of information greater than mere relevance and utility.

***Record*** - any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

***Relevance*** - limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended.

***Routine Use*** - with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

***System of Records*** - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

***Derived*** data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

***Aggregation*** of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data. (For example, tables or data arrays).

# Department of State
# Privacy Impact Assessment

## A. CONTACT INFORMATION:

**Who is the Agency Privacy Coordinator who is conducting this assessment?** (Name, organization, and contact information).

**Ms. Charlene Thomas**
**Bureau of Administration**
**Information Sharing Services**
**Office of Information Programs and Services**
**Privacy**

## B. SYSTEM APPLICATION/GENERAL INFORMATION:

**1) Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail address: PIA@state.gov If answer is yes, please complete the survey in its entirety.**

**YES _X_ NO___**

***The following are examples of personally identifiable information:**

- Name of an individual
- Date and place of birth
- Address
- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history
- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

**2) What is the purpose of the system/application?**

The American Citizen Services Plus System is used by overseas posts to record the provision of services to citizens, such as passport issuance, report of birth issuance, registration, arrests, death, etc.). It is also used by the Office of Overseas Citizen

Services to monitor status of services provided and to create financial (loan and trust) cases.

**3) What legal authority authorizes the purchase or development of this system/application?**

The system was developed and modified to support U.S. immigration and nationality law as defined in the major legislation listed below:

- Immigration and Nationality Act (INA) of 1952 (and amendments)
- 22 U.S. Code (various sections)
- 22 Code of Federal Regulations (CFR) (various sections)

## C. DATA IN THE SYSTEM:

**1) Does a Privacy Act system of records already exist?**

**YES _X__ NO___**

**If yes, please provide the following:**
**System Name _____ Number ____**

Policies/procedures governing the disclosure of American citizen information is specified various sections of 7 FAM Consular Affairs. The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

**If no, a Privacy system of records description will need to be created for this data.**

**2) What categories of individuals are covered in the system?**

**U.S. Citizens:** U.S. citizens are the primary individuals covered by this system.

**Non-U.S. Citizens:** Some non-U.S. citizen data may be collected in the process of providing services. For example, non-citizen relative information, contact information or service provider information may be collected during the process of providing services to American citizens overseas.

DoS employee information such as a name is collected and stored with the applicant's record as it relates to the auditing of actions taken during the processing of the applicant's service request.

**3) What are the sources of the information in the system?**

a. **Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**
The primary source of information is from the individual applicant.

b. **Why is the information not being obtained directly from the individual?**
In some instances, initial information for certain cases may be collected from local authorities (e.g. for an arrest or death case where the local authority may be the only source of the data)**.**

c. **What Federal agencies are providing data for use in the system?**
The Federal Bureau of Investigation (FBI) may provide data relevant to international child abduction cases.

d. **What State and/or local agencies are providing data for use in the system?**
The National Center for Missing and Exploited Children may provide data relevant to international child abduction cases. Additionally, foreign local agencies/authorities may provide data for certain types of cases (e.g., for arrests and deaths).

e. **From what other third party sources will data be collected?**
N/A.

f. **What information will be collected from a State Department employee and the public?**
Information collected from Department of State employees would be data relevant to the auditing of services provided, such as an employee name.

Information collected from the public would be data relevant to the service for which they are applying. In almost all cases, personal biographic data, such as names, dates of births, places of birth, passport numbers, addresses, contacts, etc. is collected. Biometric data, such as facial image, is collected for certain services, such as passport issuance. Additional information may be collected depending on the service requested.

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOS records be verified for accuracy?**

Data collected by other agencies and/or foreign local authorities that is provided to the Department of State is verified by civil service or FSN staff during routine processing of the service request and by a Department consular officer at the time of adjudication.

**b. How will data be checked for completeness?**
Same process as described in 3a above.

**c. Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Data collected for certain services, such as passport issuance or issuance of consular report of birth abroad, is only relevant to the processing of that application. At the conclusion of the adjudication process for that service, the applicant's record is considered "closed" and no further updates may be made. Other services, such as registration, arrests, etc. may require long term interaction with the applicant. Data will be updated as new/additional information is acquired from the citizen during routine contact.

**d. Are the data elements described in detail and documented?** If yes, what is the name of the document?

The data elements for all systems covered by this project are described in Data Dictionaries for each system.

## D. DATA CHARACTERISTICS:

**1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

**2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No.

**3) Will the new data be placed in the individual's record?**

N/A

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

N/A

5) **How will the new data be verified for relevance and accuracy?**

N/A

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Access to all systems data is controlled through the use of user roles. The same rules apply whether the user is accessing the data locally or from the consolidated database.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

N/A

8) **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data is routinely retrieved using name, date of birth, and place of birth. Depending on the system used to process the applicant's record, case numbers or applicant IDs may also be used to retrieve applicant data.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The systems covered under this program produce a wide variety of reports. The reports specific to individuals would be case reports, which list the details of a specific service. These reports would be used to review and document the details of a specific case. Only authorized users, based on the user's role, would have access to these reports.

## E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

CA employs configuration management controls over the software that is used to process applicant data. Databases that contain applicant data are under strict control of the CSD Data Engineering team who ensure data integrity and database reliability.

**2) What are the retention periods of data in this system?**

The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

**3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

**4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

N/A

**5) How does the use of this technology affect public/employee privacy?**

N/A

**6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

The system can be used to identify individuals through the use of basic biographic information. The system can be used to monitor employee activity as it relates to the auditing of the process. The system can be used to locate individuals in the event that they need to be notified of emergency situation in the consular district in which they are resident.

**7) What kinds of information are collected as a function of the monitoring of individuals?**

Auditing data, such as an employee name, is collected for the purposes of auditing the process. Access to audit reports is limited to management personnel.

**8) What controls will be used to prevent unauthorized monitoring?**

**Logs of how accessed what??**

Audit reports are available to CA management personnel **only**.

**10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No. The data processed by ACS+ has not changed.

**11) Are there forms associated with the system? YES _X__ NO ___**
**If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?**

Official forms used to collect applicant data that is entered into the systems under this program are OMB approved and contain Privacy Act statements. Specific information regarding how the data is used is contained in the Federal Register.

## F. ACCESS TO DATA:

**1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)**

The primary users that access the data are civil service personnel, Foreign Service Nationals and Foreign Service Officers in the roles of data entry clerks, consular officers, systems administrators and consular managers. Developers may have access to data for the purpose of troubleshooting the system and/or database problems.

**2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access is determined based on the user's role. User roles are assigned by the local systems administrator based on the job the employee will be performing. Only system administrators are allowed to create user IDs and assign user roles.

**3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

Users will only have access to the data granted to the role that they have been assigned.

**4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.)**

Access to data in ACS+ is determined based on the user's role. A user role may allow access to all or only partial data in an applicant's record. Some, but not all, access to records is audited. The primacy focus of audit trails is to document the actions taken in processing a particular request for service, in particular the adjudication and printing of a citizenship document.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Contract personnel are involved in the design and development of these systems. Privacy Act information is included in their contracts. All users of CA systems are required to complete the standard computer security training.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

ACS+ shares data with Passport Systems. All data sharing is for the purposes of completing the processing of the service.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Privacy rights for systems outside of ACS+, such as passport systems, will be the responsibility of the system manager, IT security manager, and/or privacy coordinator for those systems.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

Yes. Other federal agencies involved in international child abduction may have access to this data.

9) **If so, how will the data be used by the other agency?**

Other agencies use data provided by these systems for law enforcement purposes. A Memorandum of Understanding (MOU) is usually implemented between the data owner, such the Office of Overseas Citizen Services, and the agency receiving the data to define how the data will be used.

10) **Who is responsible for assuring proper use of the data?**

The recipient of the data is responsible for assuring proper use of the data as defined in the applicable MOU.

**ADDITIONAL COMMENTS:** *(optional)*